3-15.000
SECURITY
PROGRAMS MANAGEMENT

3-15.010 Introduction

Security programs which effectively protect personnel, offices, and investigative and administrative information enable the United States Attorneys' offices (USAOs) to accomplish their mission and goals. The active participation of senior management is critical to the success of these security programs. Security programs management within USAOs comprises three distinct components: the Executive Office for United States Attorneys (EOUSA), the District Office Security Manager (DOSM), and the Domestic Terrorism Working Group of the Attorney General's Advisory Committee.

A. EOUSA provides the following support for USAO security programs:

- Policy and procedural assistance for the implementation of all security programs in accordance with applicable statutes and Executive and Departmental Orders to ensure the unique needs of each office are met.
- General and specialized security training for all personnel responsible for security-related duties.
- Budgetary and facilities management support to facilitate the design, procurement, and installation of all security-related equipments, services, and systems.
- A structured methodology for analyzing the overall security practices of each USAO and determining office-unique security requirements.

- Oversight to identify weaknesses, provide assistance and advice, ensure compliance with all national and Departmental security policies and regulations, and formulate constructive recommendations to improve the overall quality of security programs and support.

B. Each United States Attorney appoints a DOSM, preferably a Supervisory Assistant United States Attorney, to manage all district security programs. As the principal security official for the district, the DOSM advises the United States Attorney on all security matters, and is assisted by other assigned individuals as required. The DOSM is responsible for:

- Analyzing the overall security posture of the district office and recommending necessary security systems, equipment, and services to reduce vulnerabilities and risks.
- Implementing and locally overseeing the physical, information, personnel, computer, and communications security programs, as well as the security education and awareness, loss prevention, and safety and health programs in accordance with current policy.
- Developing the District Security and Occupant Emergency plans.
- Preparing and submitting Urgent and Security Incident Reports.
- Preparing budget estimates for implementing office security programs, and coordinating these and other security requirements with EOUSA.

C. The Domestic Terrorism Working Group, whose membership includes United States Attorneys and Assistant United States Attorneys, is part of the Attorney General's Advisory Committee. The Subcommittee coordinates security-related initiatives and educational efforts with EOUSA.

3-15.100 Security Programs

The DOSM Handbook, which sets forth the requirements and procedures for district security programs and contains copies of applicable security regulations, has been distributed to all USAOs. Refer to the Handbook for more detailed information concerning the following security programs:

3-15.110 Personnel Security

A. Background Investigations. All USAO employees must be United States citizens, and require favorably completed background investigations (BIs) prior to entering on duty. Completed Bis are received and initially reviewed by the EOUSA Security Programs Staff. While the Department of Justice (DOJ) Security Officer, Justice Management Division (JMD), has final adjudication authority, attorney and law clerk investigations must also be approved by the Office of Attorney Personnel Management (OAPM). Favorable adjudication may not be granted, or may be delayed, if the BI reveals questionable or potentially derogatory information.

In unusual or emergency circumstances, USAOs may request a waiver for completing the BI prior to entrance on duty by submitting to the EOUSA Personnel Staff: a justification, the results of vouchering inquiries, and security forms completed by the individual. Waiver requests for attorneys and law clerks are forwarded to the OAPM for approval, and those for nonattorneys to the Department Security Officer.

Reinvestigations to update Bis are conducted for employees whose Bis are five years or older. The favorable adjudication of a BI is not commensurate with approval of a national security clearance. Any applicant or employee who may require access to classified information in the performance of their duties must execute Standard Form (SF) 86, Questionnaire for National Security Positions.

B. National Security Clearances. USAOs must contact the EOUSA Security Programs Staff to request National Security Clearances when employees require access to National Security Information, which is generally in connection with litigation involving classified information. Clearances for access to classified information can only be granted if a favorably completed BI is current (i.e., less than five years old), and the employee has a "need-to-know" the information.

Requests for access to Sensitive Compartmented Information (SCI) or Department of Energy "Q" clearances should also be initiated through the Security Programs Staff. SCI is classified information, which concerns or is derived from intelligence sources and methods, and requires strict control in accordance with Intelligence Community directives. Approval for access to SCI includes a required briefing, which must be conducted in an approved Sensitive Compartmented Information Facility. Employees granted access to SCI are required to report all foreign travel, official and personal, to the JMD in advance of their departure by submitting a completed DOJ Form-504, Notification of Foreign Travel. "Q" clearances for access to restricted information concerning nuclear weapons matters are authorized only by the Department of Energy pursuant to provisions of the Atomic Energy Act of 1954. Most departments and agencies require written certification from the Department Security Officer to confirm the national security clearances of USAO personnel attending meetings or conferences at which classified information will be discussed. USAOs should contact the EOUSA Security Programs Staff two weeks in advance, which will in turn request certification be forwarded by the Department Security Officer, JMD.

When an employee's need for access to classified information no longer exists, the USAO should advise the Security Programs Staff that the clearance may be cancelled. Employees should be formally debriefed from SCI and Q programs.

3-15.120 Information Security

Information security involves the control and safeguarding of Limited Official Use (LOU) information and National Security information (NSI). Other departments and agencies entrust LOU information and NSI to the USAOs during investigations and litigation. It is important that USAOs protect LOU information and NSI, and any materials developed using such information, in the same manner as the originators. All LOU information and NSI must be protected to prevent disclosure to individuals not authorized access to the information.

A. Limited Official Use (Sensitive) Information. Departmental policy defines LOU information, also referred to as "sensitive," and establishes procedures for its protection. LOU information includes, but is not limited to grand jury information, informant and witness information, investigative material, Federal tax and tax return information, Privacy Act information, and information which can cause risk to individuals or could be sold for profit. The information should be labeled or identified by placing the caveat "Limited Official Use" on the first page, by a notation in a covering memorandum, or by affixing an LOU label or cover sheet to the material to ensure recipients are aware the information requires protection. Provided the USAO has minimum physical security safeguards in place, sensitive information may be stored, when not in use, in locked offices, desks, or cabinets. Secure telephone and facsimile equipment should be used whenever possible to protect sensitive information, particularly investigative, informant, witness, or Title III information.

B. Tax and Tax Return Information. Although Federal tax and tax return information is generally regarded as LOU information, Section 6130 of the Internal Revenue Code and Departmental policy establish safeguards beyond those mentioned above. Access to tax and tax return information will be limited to the United States Attorney and those Assistant United States Attorneys and support staff assigned to the particular case. When in use, the information may be kept in the Assistant United States Attorney's office provided the office is locked when the Assistant United States Attorney is not present. To the maximum extent possible, tax information must

be kept separate from other information. Where separation is impractical, such files or containers should be clearly labeled to indicate they contain tax return information. If tax documents cannot be personally transmitted, the material shall be transmitted, double-wrapped, by United States Postal Service registered mail, with a return receipt to be signed by the addressee or authorized designee. The interior wrapping or envelope shall be marked "LIMITED OFFICIAL USE, TO BE OPENED BY ADDRESSEE ONLY."

The receipt and disclosure of all tax information shall be recorded on a tax information log, which also reflects the chain of custody. Tax logs must be retained for five years from date of receipt or date of any disclosure, whichever is longer. When the information is no longer needed, original tax information must be returned to the Internal Revenue Service within 90 days. Copies of tax information not made public during the course of judicial or administrative proceedings should be destroyed by shredding. Magnetic tapes containing tax information may not be made available for reuse or released for destruction without first being subjected to electromagnetic erasing.

C. Grand Jury Information. USAOS must ensure that contracts with grand jury court reporters contain current security requirements. Grand jury court reporters must be cleared and approved by the Department Security Officer, JMD, with a favorably adjudicated name and fingerprint check. These clearances must be updated every five years.

Reporters must protect grand jury information and materials in their custody from disclosure to unauthorized individuals. At a minimum, material must be secured and stored in an alarmed facility with locked entrances and exits during nonworking hours. Office automation equipment, such as word processors or personal computers, may be used to process grand jury information provided the equipment is used in a dedicated, standalone mode and the information is unclassified. During nonworking hours, diskettes and removable hard drives must be secured in approved containers. Equipment having fixed hard drives must be secure to preclude access by unauthorized individuals such as unescorted cleaning persons. Service personnel must be escorted at all times when working on or around processing equipment.

Reporters must ensure that grand jury information does not remain on storage media, and that all storage media, including fixed hard drives, is removed from the equipment before being moved from the contractor facility for maintenance, servicing, or final disposition. All removable storage media becomes the property of the government, and fixed hard drives must be made available to the government for sanitizing.

D. National Security (Classified) Information. NSI, which is also referred to as "classified information," concerns national defense and foreign relations matters. National and Departmental policies prescribe requisite procedures for marking, handling, storing, and transmitting NSI. Refer to Paragraph 3-15.100, B, for guidance on requesting national security clearances.

The following three classification levels for NSI indicate information sensitivity and the potential damage to United States national security if the information is disclosed to unauthorized individuals:

- TOP SECRET (TS) could cause "exceptionally grave damage,"
- SECRET (S) could cause "serious damage," and
- CONFIDENTIAL (C) could cause "damage."

Classified documents must be clearly marked to indicate their level, authority, and duration of classification. When not in use, classified documents and computer media on which NSI is stored must be locked in security containers ("safes"). Classified documents must be accounted for, and when no longer required, returned to the originating agency or destroyed by shredding in an approved "cross-cut" shredder.

NSI must not be processed on EAGLE or PRIME computers. Classified information must be processed and stored, following special procedures, on standalone or laptop computers.

Classified information must not be discussed or transmitted by commercial telephone or facsimile. Secure telephone (STU-III) and/or secure facsimile, keyed to the appropriate classification level, *must* be used to discuss or transmit classified information. SECRET and CONFIDENTIAL material may be sent by United States Postal Service registered or express mail, return receipt requested. TOP SECRET material cannot be mailed from office to office, but may be hand-carried by an employee possessing a TOP SECRET clearance. Any classified material which is mailed or hand-carried must be double-wrapped.

The Classified Information Procedures Act (P.L. 96-456. 94 Stat. 2025) is invoked for some cases involving NSI. In such cases, the Department Security Officer appoints a special Court Security Officer to assist the Federal Judiciary, the defense, and the USAO. EOUSA provides funding for additional security resources and equipment for such cases.

3-15.130 Computer Security

The computer security program is mandated by the Computer Security Act of 1987 (P.L. 100-235), and involves the safeguarding of information in electronic or magnetic media form and of the systems used to electronically process that information. The program focuses on the security of the PRIME Computers, word processing equipment, the EAGLE system, personal computers, laptop computers, and the information these systems store and process. This information is primarily case-related, although some administrative records relate to personnel and budgetary functions. Procedural guidance should be developed which sets forth basic computer security safeguards such as separation of functions, safety considerations, and access control and protection of USAO computer systems and equipments from misuse or computer-related crime.

Each computer system which processes sensitive or classified information must be certified and accredited. A risk analysis must be conducted for each system, and computer security and contingency plans, which allow for the continuation of automated processing in the event of natural disaster or system damage, must be prepared. Additionally, computer security software which encrypts data, protects communications, and detects viruses must be installed. The System Manager, or other responsible party, certifies that contingency and computer security plans are complete, and that safeguards are in place. The United States Attorney, or senior designee, accredits the systems by acknowledging and accepting any residual risk associated with operating the systems as configured.

3-15.140 Communications Security

Communications security (COMSEC) involves the protection of voice, data, and facsimile signals during transmission. Rapidly advancing technology and the ease with which communications systems can be monitored and exploited by criminal elements or hostile intelligence services presents a serious challenge to the legal and law enforcement community. The Type 1, Secure Telephone Unit-Third Generation (generally referred to as the STU-III) was developed in response to National Security Decision Directive 145 (1983) which mandated the production of a reliable, cost-efficient secure telephone, which could also function as a normal telephone instrument and be provided to each Federal employee whose duties entailed the discussion of *sensitive* and/or *national security (classified) information*.

The STU-III program is fully supported by the Attorney General and the Director, EOUSA. All USAOs have been furnished STU-IIIs and secure facsimile equipment in order to provide a secure means to exchange

sensitive and classified information concerning ongoing cases with other USAOs, Department components, and law enforcement entities. Secure telephone and/or secure facsimile equipment *must* be used to discuss or transmit classified information, and *should* be used to protect sensitive information, particularly investigative and informant or witness information.

Each USAO has also been provided at least one TRIAD system consisting of a secure telephone, a secure facsimile machine, and a personal computer which can be used to process sensitive and/or classified information, and directly transmit such information in a secure manner to other Department or law enforcement organizations. The STU-III program has been further expanded with the development of the Type 2 secure telephone unit for installation at state and local government and law enforcement organizations through a Federally-sponsored program.

Within each USAO, the DOSM oversees communications security and the STU-III program, determines USAO requirements for secure telephone and facsimile equipment, and promotes the use of secure communications equipment among district personnel. Primary and Alternate COMSEC Representatives will be appointed to assist the DOSM. The COMSEC Representatives are responsible for day-to-day management of secure communications equipment, maintaining required accounting records, and conducting periodic inventories of COMSEC equipment and material.

3-15.150 Physical Security

See the EOUSA Resource Manual at 131.

3-15.160 Reporting Security Incidents and Emergency Security Support

The DOSM is responsible for immediately reporting to EOUSA any situation which: (1) involves possible or actual injury to employees, (2) results in loss of, or damage to, Government assets; or (3) affects or threatens the ability of a USAO to operate. Examples of reportable incidents include: threats to a USAO or its employees, office break-ins, theft or loss of Government property, and discovery of computer viruses.

Urgent Reports are submitted to report significant events of interest or concern to the Attorney General and Deputy Attorney General. Such events include bomb threats which directly involve a USAO, threats against USAO personnel, and any natural or man-made emergency which affects the continued operation of an office. *See* USAM 3-18.200.

Security Incident Reports are submitted to report all other types of security-related incidents (e.g., bomb threats which do not directly involve a USAO, thefts of personal or Government property, disclosure of sensitive or classified information to unauthorized individuals, and discovery of computer viruses).

Submission of an Urgent or Security Incident Report initiates a variety of corrective or protective measures and should not be delayed pending the development of more detailed information. Follow-up reports may be submitted to provide additional data.

When it is first learned that a threat has been made or may exist against a USAO or an employee of a USAO, three things must be done *immediately*:

- **Notify the local United States Marshal.** When threats warrant such action, the United States Marshals Service (USMS) provides assistance to threatened individuals in the form of personal security briefings, residential security surveys, and armed protective details. The local United States Marshal reports the threat to USMS Headquarters, which compiles all threat-related data and rates the threat High, Medium, or Low

to determine if protective services are warranted. The local Marshal has the authority to assign a protective detail for 72 hours, continuances are approved by USMS Headquarters.

- **Notify the local Federal Bureau of Investigation (FBI) office.** The FBI investigates all threats made against Department employees. Upon notification, the FBI initiates an investigation and shares investigative results with the USMS, the USAO, and EOUSA.
- **Submit a report to EOUSA.** Urgent Reports, unless classified, should be submitted to EOUSA by electronic mail to AEX15(URGENT). *See* USAM 3-18.200. Security Incident Reports should be submitted to the Security Programs Staff by facsimile, electronic mail (to AEX13(SECMAIL), or telephone.

When threats to an individual or an office develop, EOUSA provides emergency security support to the USAO. The measures taken are proportional to the speed with which Urgent or Security Incident Reports are provided. The Security Programs Staff compiles and coordinates threat-related information with the USMS, the FBI, and other sources to determine the nature of emergency security support required by the USAO or individual to adequately counter the threat. This support may consist of one or more of the following:

- Providing immediate on-site surveys and assistance to the affected district, advice and assistance to threatened individuals on dealing with the threat locally, or assistance in obtaining special deputy status.
- Authorizing, funding, and coordinating the relocation of the threatened individual and/or immediate family members, the immediate installation of residential or automobile alarm systems and/or remote automobile starting devices, or the purchase or temporary lease and installation of other security-related items and equipment.

3-15.170 Deputation (Authorization to Carry Firearms)

The Deputy Attorney General (DAG) may authorize the appointment of United States Attorneys and Assistant United States Attorneys as Special Deputy United States Marshals to enable them to carry firearms in accordance with the 1988 DOJ policy pertaining to the carrying of firearms by United States Attorneys and Assistant United States Attorneys. Attorneys requesting deputation must furnish their own firearms and ammunition, and have completed USMS-approved firearms proficiency and safety training within a six-month period prior to the request. Deputation is authorized on an individual, case-by-case basis for the limited purpose of carrying firearms without violating local, state, and Federal laws. Firearms may only be used defensively as a last resort to prevent loss of life or serious bodily injury when there is imminent danger. Such deputation expressly excludes law enforcement powers such as the power to arrest for violations of federal law and court-related duties of United States Marshals.

For a discussion of the criteria involved in deputation, see the EOUSA Resource Manual at 132.

3-15.180 Occupational Safety and Health Program

The Director, EOUSA, has overall responsibility for implementing the Occupational Safety and Health Program in accordance with the Occupational Safety and Health Act of 1970 (29 U.S.C. 651 et seq.); Executive Order 12196, "Occupational Safety and Health Programs for Federal Employees"; 29 CFR § 1960, et seq., "Basic Program Elements for Federal Employee Occupational Safety and Health Programs"; and Department of Justice Order 1779.2A, "Occupational Safety and Health Program." The Director has designated the Assistant Director of the EOUSA Security Programs Staff as the Safety and Health Manager to administer the Occupational Safety and Health Program for EOUSA and the USAOs. Reports of unsafe or unhealthful working conditions should be directed to the Manager who will investigate the matter, and make every effort to ensure such matters are

corrected in a timely manner. If a condition cannot be corrected within the specified time frame, the Manager notifies the Director of the status of corrective efforts, the basis for the delay, and recommends a course of action.

Each United States Attorney shall designate an individual to serve as the district Occupational Safety and Health Coordinator. Coordinators must be afforded appropriate training and their duties incorporated into performance work plans. The Coordinator is responsible for: arranging and participating in annual inspections of district offices; monitoring findings and reports of inspections to confirm that appropriate corrective measures are implemented; reporting to EOUSA any unsafe or unhealthful working conditions; displaying the Occupational Safety and Health Act poster; conducting investigations and maintaining records of employee or public injuries, property damage, and motor vehicle accidents; and an annual summary of occupational injuries, illnesses, accidents, and property damage.

For further information on investigations and reports, see the EOUSA Resource Manual at 133.

3-15.190 Emergency Planning

Emergency planning within the USAOs encompasses two areas: 1) local emergency planning efforts which require the development of Occupant Emergency Plans and 2) national security emergency planning efforts which specify courses of action to ensure the continued operation of the Federal Government in the event certain crisis situations occur.

A. Occupant Emergency Plans. Federal Property Management Regulations, 41 CFR, §101-20, require that a short-term emergency response program be developed, and that procedures for safeguarding lives and property in Federally-occupied space during specified emergencies be established. Where the USAO is the primary tenant of a Federal building or facility, and the United States Attorney is the Designated Official, it is the DOSM's responsibility, as the United States Attorney's designee, to ensure an Occupant Emergency Plan is developed and coordinated with other occupant agencies. Where the USAO is not the primary tenant, it is the DOSM's responsibility to participate in the development and staffing of the Occupant Emergency Plan. DOSMs may contact the Security Programs Staff or their local GSA office for guidance and assistance in the preparation of Occupant Emergency Plans. In addition to ensuring that an Occupant Emergency Plan is established for each office within the district, the DOSM must ensure that all USAO employees are familiar with applicable emergency procedures. Occupant Emergency Plans should be reviewed and updated annually. DOSMs should ensure that, at a minimum, evacuation drills are conducted on an annual basis.

B. National Security Emergency Preparedness. Pursuant to Executive Order 12656, "Assignment of Emergency Preparedness Responsibilities," and in accordance with subsequent DOJ Orders, it is Department policy to maintain a high level of readiness in order to respond to any emergency (i.e., natural disaster, military attack, technological emergency, etc.) which seriously degrades or threatens national security and to ensure the continuity of the Department under such conditions. Before, during, and after such emergencies, the Department must maintain both headquarters and field capabilities to perform the following essential uninterruptible functions:

- Provide for Attorney General succession;
- Furnish legal advice to the President, the Cabinet, and the heads of executive branch department and agencies; and
- Respond to law enforcement matters including foreign counterintelligence and domestic security threats.

For the purposes of federal emergency preparedness programs, regions have been established and regional cities have been designated from which field entity emergency efforts will be directed. The United States

Attorneys in the regional cities of Boston, New York (Southern District), Philadelphia, Atlanta, Chicago, Dallas, Kansas City (Missouri), Denver, San Francisco, and Seattle are responsible for serving, in their respective regions, as the senior DOJ official and as the senior member of the DOJ Regional Emergency Team which will include representatives from the FBI, the Immigration and Naturalization Service, the Drug Enforcement Administration, the USMS, and the Bureau of Prisons. As senior Regional Team members, these United States Attorneys must ensure that all appropriate DOJ emergency plans are developed, maintained, and, in time of emergency, implemented.

Each regional United States Attorney must designate an individual within their office to serve as the Justice Regional Emergency Coordinator (JREC). The JREC assists the United States Attorney, coordinates policy implementation and operational readiness planning, and serves as liaison between the Federal Emergency Management Agency and all participating DOJ field components. All DOJ field organizations are required to establish an order of succession through a minimum level of four positions for each staffed office to include a delegation of authority. This information must be provided to the JREC. Interagency emergency preparedness training may be held periodically and may involve participation by certain USAO or other DOJ personnel.

3-15.200 District Security Plan

Each USAO is required to develop a "District Security Plan" which, at a minimum, will include certain required elements. The plan should be reviewed on an annual basis, updated as necessary, and made available to all district employees. Required elements of a District Security Plan are in the EOUSA Resource Manual at 134.

3-15.300 Security Education and Awareness

National and Departmental regulations require that employees be provided both initial and refresher security training. DOSMs should establish regular, ongoing security education and awareness programs to ensure USAO employees are familiar with their security responsibilities and USAO emergency procedures. To assist DOSMs in developing training, EOUSA distributes a wide variety of security education materials including: a quarterly security bulletin and advisory memoranda, videos, posters, pamphlets, and books concerning topics such as secure communications, computer security, bomb threats, mail bombs, workplace violence, and personal safety.

New employees should be afforded general security training during orientation. Refresher training may be accomplished by disseminating security information via electronic mail, in district newsletters, or at regular staff meetings. A number of districts have implemented a "security awareness month" during which mandatory and voluntary training sessions are held covering such issues as office security, computer security, information security, mail bombs, and personal safety. DOSMs should consider requesting guest speakers from the EOUSA Security Programs Staff, the DOJ Employee Assistance Program office, local offices of Federal law enforcement (e.g., FBI, USMS, ATF, United States Postal Inspections Service), the local police department, and community organizations such as the PTA or Neighborhood Watch.